DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350·1000

SECNAVINST 3501.2
DUSN
04 Jan 2021

SECNAV INSTRUCTION 3501.2

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY MISSION ASSURANCE PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Responsibilities
(3) Acronyms and Definitions

1. Purpose

a. This instruction implements the Department of the Navy (DON) Mission Assurance (MA) program and aligns with the Department of Defense (DoD) MA policy guidance provided in references (a) through (x). The DON MA program supports the DON Services' ability to ensure the protection and/or continued function and resilience of critical capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, utilities, and supply chains critical to the execution of DoD/DON Mission Essential Functions (MEFs) and Mission Essential Tasks in any operating environment or condition.

b. This instruction establishes an integrated and supportive MA governance structure to protect the force, provide a framework for the systematic advocacy for DON risk reduction efforts, the DON Services' ability to synchronize complementary protection-related programs and activities, and enable the prioritization of investments to ensure mission success. Guidance provided herein will also facilitate coordinated MA input into the DON Planning, Programming, Budgeting, and Execution (PPBE) process; Joint Capability Integration and Development System; and the Defense Acquisition System.

c. This instruction carries forward and re-purposes all governance structures, coordination processes, programming, resources, functions, and activities supporting responsibilities previously assigned under the DON Critical Infrastructure Protection (CIP) Program in accordance with reference (a).

d. This instruction incorporates national-level requirements related to MA identified in references (b) through (f).

e. The Deputy Under Secretary of the Navy (DUSN) is designated as the DON Office of Primary Responsibility (OPR) for DON MA Policy.

2. Cancellation. SECNAVINST 3501.1D.

3. Applicability and Scope. This instruction applies to the Offices of the Secretary of the Navy (SECNAV); the Chief of Naval Operations (CNO); the Commandant of the Marine Corps (CMC); U.S. Navy and U.S. Marine Corps installations, commands, activities, and field offices; and all other organizational entities within the DON.

4. Policy. DON MA policy includes the following primary components:

a. Strengthen the protection and resilience of critical capabilities and assets against man-made and naturally occurring threats and hazards per reference (g). Collaboration across the DON is essential to proactively manage and reduce risk to mission execution. These efforts will seek to identify and deter threats, reduce vulnerabilities, and minimize consequences while retaining the flexibility and agility necessary to plan for and respond to future protection needs. When loss or degradation of critical capabilities or assets occurs, plans will be implemented to minimize impacts and restore mission capability. Priority remediation and mitigation activities will be given to Defense Critical Assets (DCAs) and Mission Assurance Coordination Board Select Tier 1 Task Critical Assets (TCAs).

b. Implement the DoD MA Construct that supports the DON’s execution of responsibilities and missions in accordance with references (g) and (h). References (g) through (i) provide policy and guidance that supports risk management activities associated to critical assets and capabilities within the DoD.

c. Support risk-informed decision-making through a DON-wide MA governance process. An integrated MA governance structure and supporting processes will be implemented in the DON and Services-levels, including major commands directly reporting to the DON, to enable the comprehensive risk assessment and review of identified areas of risk; inform policy, plans, programs, and resource allocation; and drive actions to manage risk effectively. Within this governance structure, many risk decisions will remain decentralized at the local command level. Strategically, the DON and its Services will facilitate the management of risks that affect DON-wide mission performance; help determine priorities and economies-of-scale protection solutions; and provide risk-based inputs into the PPBE process.

(1) The key DON element of this governance structure includes the designation of the DUSN as the MA OPR for the DON and the alignment of Service MA OPRs to support a collaborative governance body for MA-related efforts.

(2) Service-level MA OPRs, executive committees, and working groups will be responsible for integrating output from the MA risk management processes and coordinating with the DON MA OPR and other stakeholders within the Department to ensure mission success. These entities will provide visibility to the DON MA OPR regarding MA capabilities, gaps, and priorities across individual resource sponsors through their chain of command on a systematic basis.

d. Better protect the force and manage mission risk through synchronization and integration between existing Service-level protection and resilience programs that support MA Related Programs and Activities, including: Antiterrorism; Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive defense; CIP; Continuity of Operations; Cybersecurity; Insider Threat, Counterintelligence; Emergency Management; Law Enforcement; Physical Security; Force Health Protection; and Energy Resilience. Although these programs may operate under separate directives, policies, and authorities, they will synchronize and coordinate under the guidance and processes established in this instruction and references (k) through (o).

e. Continue existing efforts under the DON MA policy and related program implementation to meet national-level and Defense Critical Infrastructure (DCI) requirements established in references (a) through (j). The Services may maintain existing Service-level CIP policies. The Services will maintain sufficient resources to meet DoD and DON-level responsibilities for identifying, assessing, managing, and monitoring risk to critical infrastructure and to align associated resilience and protection program risk management efforts under the MA construct. Services MA and/or CIP OPRs will continue to maintain the ability to store, handle, and share MA and DCI information in appropriate Service-level system of record up to and including Top Secret (TS) Sensitive Compartmented Information (SCI).

f. Partner with external entities to further identify, assess, and manage risk to DON missions. MA implementation will require extensive collaboration between the DON, its Services, and other DoD components; civilian government agencies; and private sector infrastructure operators, service providers, and supply chain managers. These external partners have key authorities, capabilities, and resources that are essential to the DON mission. Therefore, the DON and its Services will seek greater collaboration with these entities regarding joint risk and interdependency analyses, information sharing, scenario-based contingency and continuity of operations planning, exercises, risk mitigation, and technological innovation. The DON will encourage industry and service providers on whom it depends for mission support to design and use systems and processes that withstand disruption and address single points of failure and supply chain vulnerabilities. In addition to having access to necessary supplies and materials, supply chain concerns also include risks posed by foreign companies and components linked to adversarial nations that are part of the Service supply chain and provide necessary equipment, parts, and services required to sustain required Service functions.

5. Responsibilities. See enclosure (2).

6. Definitions. See enclosure (3).

7. Records Management

a. Records created as a result of this instruction, regardless of media and format, must be maintained and disposed of according to the records disposition schedules found on the

Directives and Records Management Division (DRMD) portal page https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office. Records created as a result of this instruction, regardless of media and format will be managed in accordance with reference (p), Part III, for the following SSICs: 3057, 3058, 3440, 3010.4, 4700, 11000, 11014, 11090, and 11100.

8. Information Management Control. The reporting requirements contained in enclosure (2), paragraphs 2c and 2d of this instruction are exempt from information collection control in accordance with reference (q), Part IV, paragraphs 7c, 7e, 7k, and 7o.

GREGORY J. SLAVONIC
Assistant Secretary of the Navy
(Manpower and Reserve Affairs)
Performing the Duties of the
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances Website:
https://www.secnav.navy.mil/doni/

REFERENCES

(a) UNSECNAV Memorandum, “Department of the Navy Critical Infrastructure Protection Program” of 1 February 2016
(b) National Security Strategy of 18 December 2017
(c) E.O. 13636
(d) Presidential Policy Directive 21 of 12 February 2013
(e) The National Military Strategy of December 2018
(f) The National Infrastructure Protection Plan of December 2013
(g) DoD Instruction 3020.45 of 14 August 2018
(h) DoD Directive 3020.40 of 11 September 2018
(i) DoD Instruction 5240.19 of 6 November 2020
(j) DoD Mission Assurance Strategy of 7 May 2012
(k) SECNAVINST 3052.2
(l) SECNAVINST 5510.37A
(m) DoD Instruction 5100.76 of 19 October 2020
(n) SECNAVINST 4101.3A
(o) SECNAVINST 5239.3C
(p) SECNAV M-5210.1
(q) SECNAV M-5214.1
(r) 10 U.S.C. §8015
(s) SECNAVINST 5430.7R
(t) SECNAVINST 5430.107A
(u) SECNAVINST 3300.2C
(v) SECNAVINST 5000.2F
(w) SECNAVINST 5500.36A
(x) SECNAVINST 3030.4E

RESPONSIBILITIES

1. The Under Secretary of the Navy (UNSECNAV) is designated as the deputy and principal assistant to the SECNAV, and acts with the full authority of SECNAV in managing the DON per reference (r). Per reference (s), UNSECNAV oversees DON critical infrastructure.

2. The CNO and the CMC will execute DON MA (including CIP) policy and assign OPRs within their respective Services to:

a. Develop, implement, and maintain MA and CIP policy to ensure the identification and validation of critical assets and capabilities, along with the assessment, prioritization, and management of risk, and protection of critical capabilities, assets, and associated supporting infrastructure per this instruction and references (g), (h), and (j). Consistent with guidance in reference (g), MA and CIP Service-levels policies may be integrated.

b. Establish a risk assessment/risk management process to include all threats and hazards, per guidance provided in references (g) and (h). This process will be designed to establish protocols for disseminating DCI-related threat assessment and hazard warnings to installation commanders, MA (including CIP) points of contact, and mission and asset owners.

c. Identify, validate, prioritize, assess, document, and manage risk to Service critical capabilities and assets in coordination with Naval Criminal Investigative Service (NCIS) in accordance with references (i) and (t).

(1) Coordinate the Critical Asset Identification Process with applicable DON MA stakeholders, including DON MA Working Group members.

(2) Document and maintain a list of critical assets and associated supporting infrastructure dependencies, per references (g) and (h), in a Service-level authoritative database and ensure the database is available to select members of the MA community on a role-based, trusted access basis.

(3) Ensure critical capabilities and assets are assessed through Service headquarters-resourced MA Assessment Teams,

including the parameters of criticality, vulnerabilities, and associated threats and hazards, to determine risk of loss, per references (g), (h), and (u) using standardized, DoD and Service-developed assessment benchmarks and methodologies.

(a) Annually, participate in the Joint Staff Integrated Assessment Conference to develop MA assessment schedules, per reference (g). Include the name of the organization that will conduct the assessment and an organization point of contact.

(b) Coordinate with Combatant Commands, via the Joint Staff Integrated Assessment Conference process, to identify and schedule critical assets and infrastructure to be assessed by existing and future processes.

d. In addition to other required reporting, within 24 hours of an event that degrades or renders a DCA or a Tier 1 TCA non-mission capable, notify the DON MA Officer of the degradation or loss and any resulting impact on associated missions by the most expeditious method available. Within 96 hours of the initial report, submit a written plan of action and milestones to the DON MA Officer, including actions taken or planned for remediation, recovery, or reconstitution. Submit monthly follow-up reports until resolved.

e. Provide Service-level input and coordination for DoD and DON MA-related policy through established tasking protocols and processes.

f. Ensure the DON MA Officer has access to DON DCA and Tier 1 TCA risk management products, e.g., assessment reports and risk management decisions.

g. Develop training and education requirements to meet the Services MA-related training standards.

3. The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN (RD&A)) will:

a. Appoint a subject matter expert(s), knowledgeable in protecting critical technologies, the Defense Industrial Base , and supply chain risk management, as the ASN (RD&A) representative(s) to the DON MA Working Group.

b. Work with the DON MA Officer and Service MA representatives to identify, characterize, prioritize, and remediate vulnerabilities to capabilities, assets, and processes managed by the acquisition community.

c. Review ASN (RD&A) policies related to or affected by MA and revise as necessary, as directed by references (g) and (v).

d. Require MA policy consideration in contracts and acquisition management procedures by incorporating requirements for the identification, prioritization, and protection of DCI in the maintenance, sustainment, and life cycles of acquisition programs.

4. The Assistant Secretary of the Navy for Financial Management and Comptroller (ASN (FM&C)) will:

a. Appoint a financial subject matter expert(s) as the ASN (FM&C) representative to the DON MA Working Group.

b. Advocate, coordinate, and provide Secretariat-level support to the Services' procedures for remediating and mitigating risks associated with mission essential financial operations.

5. The Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)) will:

a. Appoint a subject matter expert(s) knowledgeable in military and civilian policy respectively, as the ASN (M&RA) representative to the DON MA Working Group.

b. Coordinate and provide Secretariat-level support to the Services' procedures for remediating and mitigating risks associated with mission essential personnel operations.

6. The Assistant Secretary of the Navy for Energy, Installations, and Environment (ASN (EI&E)) will:

a. Appoint a subject matter expert(s) knowledgeable in public works, environmental, and energy matters, as the ASN (EI&E) representative(s) to the DON MA Working Group.

b. Advocate for MA (including integrated CIP)-related programmatic and budgetary expenditures.

c. Coordinate and provide Secretariat-level support to the Services’ MA programs to ensure:

(1) Energy, installation, and environmental activities and requirements are factored into risk assessments.

(2) Protection of energy, installation, and environmental related infrastructure that could severely impact DON missions.

d. Monitor Services’ MA (including integrated CIP) remediation and mitigation efforts.

e. Coordinate with the DON MA Officer, and Service MA OPRs and other DoD Components and Agencies to develop MA-related information sharing initiatives.

f. Ensure MA policy is considered in the review of plans and policies, including those concerning privatization and public-private ventures; make CIP policy an integral factor in directing ASN (EI&E) actions relating to facilities and utilities planning, energy security, design, construction, and maintenance.

g. Ensure Enhanced Use Leases, Energy Savings Performance Contracts, and other relevant contracts incorporate adequate security provisions to address risks posed by foreign companies and components that may be used within DON installation infrastructures and supply chains.

7. General Counsel of the Navy (GC). The GC will:

a. Appoint a representative to the DON MA Working Group.

b. Provide legal advice and counsel, as necessary or requested, to the DON MA Working Group.

8. DUSN will:

a. Serve as the Senior Executive responsible for DON Security enterprise management, accountability and oversight decisions, and make security-related resource recommendations to the SECNAV, per reference (w).

b. Serve as the DON MA Officer and the OPR for DON MA and CIP program policy, oversight, and advocacy.

c. Oversee the development, issuance, and maintenance of a comprehensive DON MA (including integrated CIP) policy and guidance.

9. The Director of NCIS as the DON Senior Official for Criminal Investigation and Counterintelligence per reference (s) will:

a. Appoint a subject matter expert(s), knowledgeable in the areas of vulnerability and threat assessments as well as indications and warning, as the NCIS representative(s) to the DON MA Working Group.

b. Provide advice, as necessary or requested, to the Department of the Navy Security Enterprise Executive Committee (DON SE EXCOM) on investigative, law enforcement, antiterrorism, technical surveillance countermeasure, and counterintelligence programs within the DON in accordance with reference (w).

c. Partner with the Office of Naval Intelligence and Marine Corps Office of the Director of Intelligence, and in coordination with DUSN and the DON Special Access Program Central Office, develop an indications and warnings capability for threats to critical infrastructures and assets per references (i) and (t).

d. Prepare and provide validated counterintelligence products as required in order to carry out CIP responsibilities on Navy or Marine Corps-owned DCI to be monitored for threats per references (g) and (i).

e. Upon request, assist Service MA assessment teams in the identification of threats to critical assets and supporting infrastructure in the development of localized All Hazards Threat Assessment per reference (t).

10. The DON Chief Information Officer (CIO), as the DON's senior official for Information Management, Information Technology and matters involving Cybersecurity will:

a. Appoint a subject matter expert(s) as the DON CIO representative(s) to the DON MA Working Group.

b. Review DON CIO policies related to or affected by MA and revise as necessary.

11. The Surgeon General/Chief Bureau of Medicine and Surgery (BUMED) will appoint a subject matter expert(s), knowledgeable in the area of health-related threats and vulnerabilities to include pandemic planning, joint blood programs and integration with off-installation health care centers, as the BUMED representative to the DON MA Working Group.

12. The Senior Director for Security and Intelligence, under the direction and control of the DUSN, will:

a. Serve as the DON Deputy MA Officer for DON MA and integrated CIP policy implementation.

b. Conduct periodic reviews of Services MA and CIP programs, including:

(1) Maintain awareness of risk management of Service-level DCAs and Select Tier 1 TCAs, including assessment reports and risk management decisions, to inform DON advocacy for resources necessary to reduce risk to the assets and their supported missions.

(2) Observe Services assessments of critical assets.

c. Conduct periodic review of Secretariat-level organizations performing MA and CIP functions.

d. Convene a DON MA working group as necessary, to coordinate DON MA efforts among stakeholders.

e. Provide appropriate representation to the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security (OASD (HD&GS)) and other federal agencies for matters pertaining to MA policy and resource advocacy. Examples include, but are not limited to:

(1) Reviewing DoD and other federal MA and related program policy in order to coordinate with the Services to develop a DON position.

(2) Advocating for MA and CIP program resources as requested by the Services.

(3) Forwarding DON DCA points of contact information to the OASD (HD&GS).

(4) Notifying OASD (HD&GS) of any event that degrades or destroys a DCA and the resulting impact on Navy and Marine Corps missions.

f. Support Service-level collaboration with the MA and DCI community to resource information sharing efforts and ensure effective security controls, processes, and procedures are implemented and maintained by repositories requesting Navy and Marine Corps critical asset data. Collaborate with Service-level MA OPRs to establish requirements to maintain and share MA data and documentation with authoritative database. Support electronic data sharing when effective, efficient, and non-duplicative actions are feasible and do not create a manpower or resource burden on the Services. This includes advocating for a single data sharing capability that:

(1) Provides for secure storage of DON MA-related classified authoritative data and documents that cannot be edited or shared without Service approval up to, and including, TS (SCI) classification.

(2) Is fully interoperable with existing DON system of record databases and all elements of information to ensure accuracy of authoritative data.

(3) Includes functionality to capture, monitor, analyze, and share critical asset risk reduction planning and implementation efforts.

g. Coordinate with the Office of the ASN (RD&A) to ensure that requirements for the risk management of DCI are identified for incorporation into acquisition, maintenance, and sustainment contracts per references (h) and (v).

13. The DON SE EXCOM is responsible for providing senior-level coordination and support to the DON MA (and integrated CIP) enterprise in order to maximize effectiveness and efficiency, and to promote strategic alignment of efforts throughout the DON. As required, the DON SE EXCOM will provide recommendations regarding the governance, implementation, and execution of DON MA policy in accordance with reference (w).

14. The DON MA (including integrated CIP) Working Group is the primary working level advisory forum for the development, vetting, and coordination of MA related policies, procedures, and actions.

a. The Working Group will be chaired by the DON Deputy MA Officer, with membership comprised of subject matter experts at grades O-5/O-6 or civilian equivalent level from all organizations listed in reference (w) and this instruction. The Working Group will convene as necessary to support DON MA-related program initiatives as provided in references (a) through (j), and (t) through (w).

b. Additional related DON working groups may be convened in conjunction with and in support of the DON MA Working Group.

ACRONYMS AND DEFINITIONS

Acronyms:

ASN (EI&E)	Assistant Secretary of the Navy for Energy, Installations, and Environment
ASN (FM&C)	Assistant Secretary of the Navy for Financial Management and Comptroller
ASN (M&RA)	Assistant Secretary of the Navy for Manpower and Reserve Affairs
ASN (RD&A)	Assistant Secretary of the Navy for Research, Development, and Acquisition
BUMED	Bureau of Medicine and Surgery
CIP	Critical Infrastructure Protection
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DoD	Department of Defense
DON	Department of the Navy
DON SE EXCOM	Department of the Navy Security Enterprise Executive Committee
DUSN	Deputy Under Secretary of the Navy
GC	General Counsel of the Navy
MA	Mission Assurance
MEF	Mission Essential Function
MET	Mission Essential Task
NCIS	Naval Criminal Investigative Service
OASD (HD&GS)	Office of the Assistant Secretary of Defense for Homeland Defense and Global Security
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
PPBE	Planning, Programming, Budgeting, and Execution
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SE EXCOM	Security Enterprise Executive Committee
TCA	Task Critical Asset
TS (SCI)	Top Secret (Sensitive Compartmented Information)
UNSECNAV	Under Secretary of the Navy

Definitions:

1. Asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public or private sector organizations. (Source: reference (h))

2. Asset Owner. The DoD Component or subcomponent with PPBE responsibility for a DoD asset, or organizations that own or operate a non-DoD asset. (Source: reference (g))

3. Chemical, Biological, Radiological, and Nuclear Defense. Measures taken to minimize or negate the vulnerabilities to, and/or effects of, a chemical, biological, radiological, or nuclear hazard or incident.

4. Continuity of Operations. An internal effort within each DoD Component to ensure that essential functions continue to be performed during disruption of normal operations. (Source: reference (x))

5. Critical Asset. Synonymous with TCA. See “Task Critical Asset” below.

6. Critical Asset Identification Process. For the purpose of this instruction, a common analytical framework that is consistent and repeatable for use in identifying TCAs and DCAs through analysis and appropriate collaboration.

7. Critical Infrastructure. Synonymous with DCI. See “Defense Critical Infrastructure” below.

8. Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the man-made or natural risks to critical infrastructure and key assets.

9. Criticality. For the purpose of this instruction, a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD or DON operations and the ability of the DoD or DON to fulfill its missions.

10. Cyberspace Security. Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

11. Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DoD to fulfill its missions. (Source: reference (h))

12. Defense Critical Infrastructure (DCI). The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of TCAs and DCAs.

13. Department of the Navy Security Enterprise Executive Committee (DON SE EXCOM). The senior-level governance body responsible for administration, strategic guidance, and policy authority for the DON Security Enterprise. (Source: reference (w))

14. Force. 1. An aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof. 2. A major subdivision of a fleet.

15. Force Protection. Preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information.

16. Hazard. A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.

17. Mission Assurance. A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the performance of DoD MEFs in any operating environment or condition. (Source: reference (h))

18. Mission Essential Functions (MEF). Select functions directly related to accomplishing the Department's mission. Failure to perform or sustain these functions, which directly support Primary Mission Essential Functions, would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control.

19. Mission Essential Task (MET). Tasks based on mission analysis and approved by the commander that are necessary, indispensable, or critical to the success of a mission.

20. Mission Owner. The OSD or DoD Component having responsibility for the execution of all or part of a mission assigned by statute or the Secretary of Defense. (Source: reference (h))

21. Mitigation. Actions taken in response to a warning, or after an incident occurs, that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (Source: reference (h))

22. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

23. Protection. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.

24. Reconstitution. The process by which surviving and/or replacement organization personnel resume normal organization operations.

25. Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. (Source: reference (h))

26. Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. (Source: reference (h))

27. Risk Assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks. (Source: reference (h))

28. Risk Management. A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. Risk management is composed of risk assessment and risk response. (Source: reference (h))

29. Risk Response. Actions taken to remediate or mitigate risk, or reconstitute capability in the event of loss or degradation. (Source: reference (h))

30. Service(s). The term "Service", "Services", "DON Services" are used as a generic term for the U.S. Navy and U.S. Marine Corps.

31. Task Critical Asset (TCA). An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or MET it supports. TCAs are used to identify DCAs. (Source: reference (h))

32. Threat. An adversary having the intent, capability and opportunity to cause loss or damage. (Source: reference (h))

33. Vulnerability. A situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources from a threat or hazard. It includes the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a threat or hazard. (Source: reference (u))

34. Vulnerability Assessment. A DoD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a threat or hazard. (Source: reference (u))